Legislative Audit Division

The University of Montana – Missoula

Information System Audit
August 2004
04DP-03

Executive Summary Administration of The University of Montana (UM) - Missoula's information technology as it relates to the Banner application, is the responsibility of the Computing and Information Services (CIS) department. Financial aid, human resource, and financial data is processed using the Banner system. Banner is a commercial software application developed by SunGard Systems and Computer Technology Corporation (SCT) and is a product used by higher education entities for managing their business processes.

The network and its security provide the foundation for all systems and software applications and, therefore, is central to all of The UM - Missoula's business goals, requirements, and operations. CIS controls the network, including managing central equipment and operations. However, security for some aspects of the network is distributed among CIS and business process owners, because The UM - Missoula business process owners control and administer hardware, such as servers and desktops, residing on the network.

We audit selected The UM Banner processes approximately every two years to understand the control environment. The current audit scope is based on specific control testing requested by Legislative Audit Division Financial-Compliance staff and specific general controls testing determined relevant to the Banner application. We performed audit work on The UM – Missoula campus to meet three objectives: 1) to provide assurance over key Banner application controls identified by Financial-Compliance audit staff, 2) to evaluate the general controls environment where the Banner application resides, and 3) to review the security administration over the network environment and assess the security of selected workstations residing on the network.

Summary The audit was conducted in accordance with Government Auditing Standards published by the United States Government Accountability Office. The current report contains three recommendations addressing:

1. Inadequate environmental conditions created by the existence of water sources near Banner backup equipment, network equipment, and power cabling

2. Excessive physical access to the computer facility housing Banner backup and network equipment

3. Compliance with Board of Regents policy by identifying security issues and exposures and developing polices addressing those concerns and designating an information security manager

In addition to this report, we provided a technical memorandum to the Legislative Audit Division Financial-Compliance staff providing results of key Banner application control testing for consideration during financial audits.